Advice on Completing Exhibit 300 Capital Asset Plan and Business Case

What is the purpose of this guidance?
This guidance provides suggestions for the acceptable completion of the Exhibit 300 Capital Asset Plan and Business Case. Instructions for completing the Exhibit 300 along with criteria for assessing its completeness are in OMB Circular A-11, Part 7, *Planning, Budgeting, Acquisition, and Management of Capital Assets* at *http://www.whitehouse.gov/omb/circulars/index.html.*

Overall

Who is responsible for the business cases?
The Exhibit 300 is the responsibility of the Project Manager and his/her CIO and should therefore be reviewed at those levels.

What if the question is not appropriate or is not answerable?
Don't leave blanks or indicate N/A. State why the information isn't available or the date/milestone after which the information will be known.

What is OMB's basis for determining if a project is high risk?
The basis for OMB scoring is the Exhibit 300 scoring criteria in OMB Circular A-11 Part 7/Section 300 pages 11 – 14 (July 2002 edition). Projects averaging less than 3 across all scoring criteria are deemed high risk, as are projects scoring 3 or below in the areas of program management or security.

Part I. Title and Screening (Yes/No) Questions

Is it ok to have an Exhibit 300's funding split on the Exhibit 53 into multiple projects or mission areas?
No, OMB requires that each Exhibit 300 have a unique user id that refers to only one project on Exhibit 53. If a project falls into two or more mission areas, OMB's guidance is to keep all the funding under the most important mission area for that project.

What if the answer is uncertain?
When in doubt, ask your CIO. It is likely in his/her area of responsibility.

When is a project a "mixed life cycle" type?
If a project covers two or more project phases (concept, planning, full acquisition, and steady state) in the same year then it is "mixed." By definition any project identified as mixed type would have funding under two or more phases of the summary spending table (where development is equivalent to full acquisition and maintenance is equivalent to steady state).

How do I know if the project is covered by GPEA?
If you are uncertain whether your project is included under the Government Paperwork Elimination Act (GPEA) provisions regarding information collection from the public, contact your bureau's GPEA Coordinator or Diana Hynek at dhynek@doc.gov.

How do I know if the project has had a Privacy Impact Assessment and what does it involve?
Contact your Privacy Officer who can verify if there is a privacy impact assessment on file. PIA is relevant for developing new systems or modifying existing systems that involve the collection, access, use, or dissemination of personal information. The system project manager should plan and budget for a Privacy Impact Assessment (PIA) during system development and coordinate the assessment with the Department's Privacy Officer and the Office of General Counsel. A PIA is a plan to build privacy protection into new information systems, for example, by asking systems personnel and program personnel to work through questions on data needs and data protection before the system is developed. The IRS PIA, which the Federal CIO Council voted a best practice, is available for reference at http://www.cio.gov/Documents/pia_for_it_irs_model.pdf.

How do I know if the project has been reviewed as part of GISRA or FISMA?
GISRA is now FISMA. Under this legislation, all IT systems and IT security programs must be periodically self-assessed using guidance in NIST Special Publication 800-26, "Security Self-Assessment Guide for Information Technology Systems" (http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf). Contact your operating unit's IT Security officer to verify if the project has been reviewed for FISMA compliance.

How do I know if the project is considered a national critical, mission critical or operations critical asset?
A project is considered a national critical asset if its failure or inability to function will result in an adverse national impact. One example is a project that is critical to the National Weather Service's capability to provide weather products to the world. The DOC Security Office maintains a list of national critical assets. Contact your IT Security Office for specific information.

"Mission critical" means that a system's failure to function would incapacitate an operating unit or agency. For example, if the system failed, a bureau would be unable to perform its agency-wide mission.

"Business critical" means that a system's failure to function would incapacitate a particular organization within an agency. For example, the HRM dept within an agency would be unable to operate but it wouldn't stop the overall bureau from performing its mission.

How do I calculate the percent funding for IT Security?
Estimate the full cost of preventing unauthorized access. This may include the estimated portions of programs/functions/applications where security is an embedded cost. Be sure

to include a non-zero value. A zero percent response will indicate that the system is not secure.

Part I. Summary of Spending for Project Stages Table and Life Cycle Budget & Financing Table

Should funds received from or provided to other agencies be reported?
I-TIPS uses the funding information from these tables to generate the Exhibit 53. To avoid double-counting OMB directs federal agencies not to include funds (reimbursable or otherwise) received from other agencies in these tables. Do report IT funding sent to other agencies. Total multi-agency funding for the project should be described in Section I.B.7.

What if funding comes from more than one appropriation account within a bureau?
Identify the appropriation account name, number, and annual amount. Annual total from all sources must equal the annual totals on the summary of spending table.

What if funding come from more than one budget line?
Identify in the Initiative Summary Sheet the account/sub activity and line item/program(s) providing funding along with the amount of funding provided from each source to the project. Save this Initiative Summary Sheet in the resource library in the project's I-TIPS folder.

I.A. Project Description

Should the description focus on the technical solution or the project's purpose?
Focus on what problem this project solves and how the solution is linked to measurable improved outcomes. The intended audience is people whose familiarity with the program/function is largely limited to this description.

What goes under the Assumption section?
Describe what resources need to be available or activities need to be accomplished that are outside the scope of this project in order to achieve this project's goals.

What is appropriate supporting documentation?
Cite third party studies or other research that identified the needs and/or verifies the appropriateness of the proposed solution. Where possible, provide dates when supporting documentation was completed.

I.B. Justification

What is the President's Management Agenda (PMA) cited in OMB's scoring criteria?
The PMA priorities are strategic management of human capital, competitive sourcing, improving financial performance, expanded electronic government, integrating budget

and performance and better R&D investment criteria. The project/function should clearly support at least one of the PMA goals. For detailed information go to the OMB Website www.whitehouse.gov/omb/budintegration/pma_index.html

What/where are the PART recommendations that projects are supposed to contribute to meeting?
Over the next few years OMB plans to review all governmental agencies using the Program Assessment Review Team (PART) process. Ten Commerce programs were reviewed during CY 2002 including MBDA, NIST/ATP, NIST/MEP, ESA, EDA, NOAA/NWS, NOAA/NMFS, PTO/Patents and PTO/Trademarks. The PART recommendations are part of the FY 2004 President's Budget and can be viewed at http://www.whitehouse.gov/omb/budget/fy2004/pma.html

I.C. Performance Goals and Measures

What if the only tangible achievements are historical?
Focus primarily on future performance targets, not past achievements

How many measures are needed during the project life cycle?
Include at least two measures for each year. The year shown is the year the target (actual performance improvement and actual performance metric) is supposed to be achieved.

What does strategic goal refer to?
Cite current Department or Operating Unit Strategic Goal.

What is meant by baseline?
It is a specific quantifiable measure that will be compared against the planned and actual performance metric, for example "10 minutes."

What is meant by performance improvement goal?
Describe the metric in narrative terms, example "Improve Tornado Warning Lead Times"

I.D. Program Management

How will increased federal government emphasis on program management effect scoring criteria and expectations?
For the FY 2005 process, OMB has said that it will fail any project that scores a 3 (of 5) or below in this area.

What information should we provide besides names?
Highlight program managers' experience and program management certification and emphasize the skills held by various members of the integrated project team.

What if the Program Manager doesn't have program management certification?
If the Program Manager doesn't have certification, then describe what training he will receive to achieve that goal. Identify and initiate project management teams, sponsors and project management training *now* if you haven't yet done so, so you can answer affirmatively to all the questions in this section.

I.E. Alternatives Analysis

Is a cost-benefit spreadsheet template available?
Yes, a spreadsheet template is in the ITIPS Resource Library under the folder entitled Cost Benefit/EVA

What if there are more than 3 alternatives?
OMB only wants, and ITIPS only accepts, 3 alternatives. Examples: buy-it, out source it, or build-it yourself; another set is status quo, incrementally improve, or totally rebuild. Meld and summarize choices to show 3 distinct alternatives.

How do I account for all the projects segments?
Some organizations price each alternative's cost by project segment such as planning, requirements definition, design, development, implementation, and operations.

What is meant by cost element?
Examples: government personnel, vendor services, vendor personnel, hardware/equipment, software, inter-agency services, supplies/other.

What is needed besides the financial comparison in choosing among alternatives?
Incorporate issues such as risk, mission contribution and timeliness in addition to financial criteria.

Which Return on Investment (ROI) measure should I use?
There are numerous ROI formulas that are used to evaluate projects. The most common are ROI %, net present value, pay back period, and internal rate of return. Use the ROI that makes the most sense for your operating unit's time horizon and investment criteria. The most common measure used in response to this question is the ROI % [(Discounted benefits – discounted costs)/ discounted costs] x 100.

Which cost/benefits are included?
Do not include sunk costs (costs incurred before the project is scheduled to begin).

What are the appropriate discount factors?
For the latest guidance see OMB Circular A-94 www.whitehouse.gov/omb/circulars/index.html. As of January 2003 the discount rate was 3.6% for five-year projects and 7% for estimated societal costs and benefits.

I.F. Risk Inventory

What risk assessment factors need to be addressed?
Address all 19 risk areas/factors listed in the Exhibit 300 instructions

I.G. Acquisition Strategy

What if the project involves multiple contracts or task orders?
For FY 2005 the Exhibit 300 is being revised to apply explicitly to each task orders or contract associated with the project. A critical component of the acquisition strategy is incorporating performance based contracting.

I.H Project and Funding Plan

Can I name ITIPS as my Earned Value Management System (EVMS)?
This section captures a high level summary of an EVMS process. ITIPS is NOT a substitute for developing an earned value management process appropriate for your project's scale. The Department is developing an EVM template for interested project managers.

How do I know whether the software program I'm using qualifies under the ANSI Standard 748?
Standard 748 refers to a process rather than a software package. A number of software vendors claim that their software is compliant. There is controversy as to whether MS Project meets the ANSI Standard; one criticism is that the baseline can be changed. But, there are third party products designed to extend MS Project's ability to meet complex earned value management needs. In the FY 2004 cycle OMB gave a top score in the Performance Based Management System category to an Exhibit 300 that cited MS Project as its EVMS software but, in addition, included considerable detail on the project's EVMS process/planning structure.

What is meant by original baseline?
Original baseline is the latest OMB approved project plan.

What if the project is on schedule but the EVMS funding amounts are different than the budgeted amount?
A proper EVM system tracks funding based on accruals, however, Exhibit 300 calculations and variances are based on Budget Authority. In some cases this discrepancy may be a justifiable explanation for an ITIPS calculated variance.

Have all the ITIPS' EVM formulas been verified?
Yes, all the formulas have been verified. One problem is that ITIPS defines BCWS as the estimate at completion. This is supposed to be fixed in ITIPS II, which is scheduled to be operational this summer.

Can ITIPS' Earned Value Analysis shows a significant variance even if the project is on schedule?
ITIPS' calculated variances assume a linear rate of spending throughout the project lifespan. At certain times this may result in the mistaken appearance of a positive or negative variance if the planned spending for that project segment is non-linear.

Part II. Additional Business Case Criteria for Information Technology

Section II.A. Enterprise Architecture

II.A.1 Business

Is this project identified in your agency's enterprise architecture? If not, why?
A fully developed Enterprise Architecture (EA) contains a "Current or As Is" architecture, a "Target or To Be" architecture, an analysis of the differences between the two (Gap Analysis), and a plan on how to close the gap and achieve the target goals (Migration Plan). New projects should be described as part of the Migration Plan.

Explain how this project conforms to your departmental (entire agency) enterprise architecture?
An EA has goals, and principles, as well as a Technical Reference Model (TRM) and Standards profile. In order for a project to conform to the EA, it must support one or more of the Architecture Goals, conform to the Architecture Principles, and conform to the TRM.

Identify the Lines of Business and Sub-Functions within the Federal Enterprise Architecture Business Reference Model that will be supported by this initiative.
The Federal Enterprise Architecture Business Reference Model (http://www.feapmo.gov/feabrm.htm) is designed to categorize all activities of the Federal Government into well-defined lines of business. These lines of business are based on function and not organization. Each line of business is subdivided into additional categories to delineate sub-functions within the primary line of business. A simple statement of the Line of Business and sub-functions involved is all that is needed.

Was this project approved through the Enterprise Architecture (EA) Review committee at your agency?
Cite the review conducted within your operating unit or the review conducted by the Commerce IT Review Board.

What are the implications for the agency business architecture?
An EA should continually evolve. Every new project should impact the business architecture, changing it for the better. It would be difficult to defend the need for a project that had no such impact.

II.A.2 Data

What types of data will be used in this project?
A project may often use several different types of data, such as financial, statistical, geospatial, etc.

Does the data needed for this project already exist at the Federal, State, or Local level? If so, what are your plans to gain access to that data?
Where possible, existing data should be used at the source, not replicated and used locally. Access to the data may require interfaces to existing systems, which involve not only the technical solutions but also all security and privacy considerations

Are there legal reasons why this data cannot be transferred? If so, what are they and did you address them in the barriers and risk sections above?
Legal reasons typically include privacy and security concerns that are specifically documented either by law, regulation, or directives from the White House or OMB.

What is spatial data and OMB Circular A–16?
Spatial data refers to data used to generate maps of various types as well as geographical information systems. The OMB Circular A-16 (http://www.whitehouse.gov/omb/circulars/a016/a016_rev.html) requires that such systems adhere to adopted standards to maintain the accessibility of the data and allow exchange of the data with other systems.

II.A.3 Application and Technology

What should be included in discussing the project's relationship to the application and technology layers of the EA?
This discussion should include the number and types of servers and the operating system to be used, the software products used to deploy the application (indicate if it is a COTS or custom developed application), as well as the network infrastructure used to deploy the application. It should also include the type of system architecture used (client/server, Web based, n-tier, host based, etc) and how the end users access the application.

Are all of the hardware, applications, and infrastructure requirements for this project included in the EA Technical Reference Model?
The Technical Reference Model (TRM) and associated Standards Profile describe in detail the requirements for the various software, hardware, and telecommunications components of the EA. To be compliant with the TRM, a product must at least meet the requirements of all applicable standards, otherwise it is not an "approved" product.

Section II.B Security and Privacy

What information should be addressed in Section II.B of the Exhibit 300?
Describe the system security controls in familiar terms – preferably the terms used in NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems* (http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf). This guidance describes security in terms of three control areas (Management, Operational, and Technical) that comprise the 17 critical element areas (see NIST Special Publication 800-26, section 3.2, pages 9-11). You may use the three control areas and/or the 17 critical elements to describe more specifically your planned and implemented efforts. Specifically,

- Question II.B.1: Explain how security is provided and funded for the project. Include a description of the key security controls. These controls should be described briefly, either by the overall control areas (Management Controls, Operational Controls, and Technical Controls) or by selecting key critical elements from the list of 17 critical elements in. Select elements that are not discussed in section II.B.2. For example, under Management Controls, describe the process for periodic review of security controls (critical element 2) and how security is considered in the project's life cycle (element 3). Under Operational Controls, describe the process for physical and environmental protection (element 7), production controls (element 8), and contingency planning (element 9). For Technical Controls, describe how identification and authentication provides security (element 15).

- Question II.B.2 and sub-questions A through F: Provide clear, descriptive, and concise responses to each question, instead of referring to a system security plan. For example:

(Either get rid of the dashes before some of the paragraphs below, or put them on all paragraphs. I don't know Word well enough to adjust this properly.)

II.B.2.A: An up-to-date security plan is one that was revised after the last major system update or within three years of the current date, whichever is more recent. If a plan exists, provide its date and whether the plan complies with requirements of OMB and NIST guidance namely OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources* http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html), and NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, (http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF). If an up-to-date, compliant plan does not exist, explain why and provide the target completion date for the plan.

II.B.2.B: State whether the project/system has undergone certification and accreditation. Specify the methodology used for certification and accreditation – DOC requires use of the National Information Assurance Certification and Accreditation Process (NIACAP), and recommends supplemental implementation guidance issued by NIST in Special Publication 800-37, *Guidelines for the Security*

Certification and Accreditation of Federal Information Technology Systems (http://csrc.nist.gov/sec-cert/SP-800-37-v1.0.pdf). Specify the title of the program official serving as the designated approving authority (DAA). State whether or not a certification was completed, and if the system has received full or interim accreditation to operate. If certification and accreditation was completed, provide the date of the accreditation. If certification and/or accreditation is not complete, explain why and provide the target completion date for certification and accreditation.

II.B.2.C: State whether the project's management, operational, and technical controls have been tested for effectiveness. Describe whether OIG, GAO, or the DOC Compliance Review Program has audited the project. Such audits examine and test the effectiveness and adequacy of management, operational, and technical controls in accordance with GAO's Federal Information System Controls Audit Manual. Also, describe all internal self-assessments performed (e.g., quarterly vulnerability scans, completion of the NIST 800-26 self-assessment checklist annually, etc.).

II.B.2.D: State whether system users have completed training in general IT security concepts as well as system specific security training. Describe the nature of the IT security training provided (e.g., Web-based training, read-and-sign agreements, warning banners on system logon) and its frequency. DOC requires general IT security training at entry-on-duty, and annual refresher training thereafter. System-specific training and update of user agreements are the determination of the system owner. Describe any user manuals developed and distributed to system users, and specify whether training includes briefing users on the system rules of behavior and consequences of non-compliance.

II.B.2.E: Describe how incident handling capabilities have been designed into the project. DOC recommends a three-pronged response that addresses prevention, detection, and correction/resumption:

> First, describe the implementation of specific operational and technical controls that detect intrusions into the project/system's computing environment, and how such detections are handled. Begin with a statement that security is a priority, therefore controls have been strengthened, implemented, or are planned to prevent the opportunity for intrusion (cite one or two examples).
>
> Next, describe the detection capabilities in terms of established policies and procedures (provide dates issued and topics covered), use of audit logs (describe key events captured and frequency of review), technical devices (type of intrusion detection sensors installed and frequency of monitoring). Add that incidents are reported to the DOC Computer Incident Response Team (CIRT), or an operating unit-specific CIRT, which in turn reports incidents to the Federal Computer Incident Response Center (FedCIRC).

Conclude by describing the procedures in place to recover from minor and major interruptions in service or loss of data after an incident has been detected, isolated, and terminated, as well as the frequency of testing the recovery plan.

II.B.2.F: Specify whether contractors operate the system, and, if so, from on-site or off-site. If contract services are included in system support, DOC requires application of Commerce Acquisition Manual (CAM) section 1337.70, *Security Processing Requirements for On-Site Service Contracts*, and related CAM Notice 00-02 (http://oamweb.osec.doc.gov/app/cam.htm). These provide facility access criteria and contract language for IT service contracts. In addition, DOC recommends use of National Institute of Standards and Technology (NIST) Special Publication 800-4, *Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials*, which provides additional guidance for security considerations in procurements.

- Question II.B.3: State whether the project permits public access. If the project permits public access, describe the operational and technical controls in place to protect privacy (also see the earlier Q&A on "Privacy Impact Assessment").
- Question II.B.4: State whether the system collects, uses, processes, transmits, or stores personal information. If so, state the reason and describe the policies and procedures in place to ensure the proper handling of personal information.

What if I need more help in preparing Section II.B of the Exhibit 300?
Consult with the system and IT security professionals knowledgeable with your specific project. In addition, your IT Security Officer and DOC OCIO's IT Security Program Team can assist you in responding to these questions.

What if I have additional questions regarding the Exhibit 300 or I-TIPS?
If you have questions regarding this advice or need related assistance on using I-TIPS to complete an Exhibit 300, please contact Stuart Simon at 202-482-0275.